NPS-OR-12-003

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DIFFERENTIAL EQUATION MODELS FOR SHARP THRESHOLD DYNAMICS

by

Harrison C. Schramm
Nedialko B. Dimitrov

August, 2012

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From-To)*
01-08-2012	Technical Report	01-10-2012 – 01-08-2012

4. TITLE AND SUBTITLE

Differential Equation Models for Sharp Threshold Dynamics

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Harrison C. Schramm and Nedialko B. Dimitrov

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
Naval Postgraduate School
1 University Circle
Monterey, CA 93940

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-OR-12-003

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES
The views expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense or the US Government.

14. ABSTRACT

We develop an extension to differential equation models of dynamical systems to allow us to analyze probabilistic threshold dynamics that fundamentally change system behavior. We apply our novel modeling approach to two cases of interest: a model of cyber infection, where a detection event drastically changes dynamics, and the Lanchester model of armed conflict, where the loss of a key capability drastically changes dynamics. We derive and demonstrate a step-by-step, repeatable method for applying our novel modeling approach to an arbitrary system, and we compare the resulting differential equations to simulations of the system's random progression. Our work leads to a simple and easily implemented method for analyzing probabilistic threshold dynamics using differential equations.

15. SUBJECT TERMS
Differential Equations, Markov Population Process, S-I-R Epidemic, Lanchester Model

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Harrison Schramm
Unclassified	Unclassified	Unclassified	UU	38	**19b. TELEPHONE NUMBER** ***(include area code)*** 831-656-2358

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL

Monterey, California 93943-5000

Daniel T. Oliver
President

Leonard A. Ferrari
Executive Vice President and
Provost

The report entitled "*Differential Equation Models for Sharp Threshold Dynamics"* was prepared for and funded by the Naval Postgraduate School.

Further distribution of all or part of this report is authorized.

This report was prepared by:

Harrison Schramm
CDR, USN
Department of Operations Research

Nedialko Dimitrov
Assistant Professor
Department of Operations Research

Reviewed by:

Ronald D. Fricker
Associate Chairman for Research
Department of Operations Research

Robert F. Dell
Chairman
Department of Operations Research

Released by:

Jeffrey D. Paduan
Vice President and
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

We develop an extension to differential equation models of dynamical systems to allow us to analyze probabilistic threshold dynamics that fundamentally change system behavior. We apply our novel modeling approach to two cases of interest: a model of cyber infection, where a detection event drastically changes dynamics, and the Lanchester model of armed conflict, where the loss of a key capability drastically changes dynamics. We derive and demonstrate a step-by-step, repeatable method for applying our novel modeling approach to an arbitrary system, and we compare the resulting differential equations to simulations of the system's random progression. Our work leads to a simple and easily implemented method for analyzing probabilistic threshold dynamics using differential equations.

THIS PAGE INTENTIONALLY LEFT BLANK

1 Introduction

Differential equation models have wide applicability in the study of dynamic systems. They are attractive because they are fast, tractable, and transparent in the sense that it is easy to understand how the inputs directly relate to the outputs. The focus of our research is to consider how differential equation models may be used to model systems with stochastic, sharp thresholds. An example of a system with a sharp threshold is a computer network where malicious code is introduced, subject to probabilistic detection and subsequent eradication. In this system, one instant the malicious code is undiscovered, and the following instant it is discovered; discovery defines the sharp threshold change in system dynamics. For a cyber infection system, statements such as "half discovered" are misleading as they do not refer to any realizable state of the system.

A sharp threshold may also be seen in a combat model where loss of a single key capability results in a change in combat dynamics. A practical example may be seen in naval combat, where the loss of a capital ship, such as an aircraft carrier, may be considered a threshold event. Statements such as "half sunk" do not refer to a realizable state of the system; however, statements about the probability distribution of a carrier surviving have meaning.

The current method of handling dynamical systems with sharp thresholds is to appeal to simulation of the threshold event by simulating the entire system's random progression. This is useful because it is easily understood, but is expensive, both in terms of computation and time. Often, many simulations are required to analyze the average behavior of the system and derive intuition about its development.

It seems that the threshold process and the differential equation model are irreconcilable, chiefly because the threshold event is not divisible in the sense that its expected state is generally not reachable. We overcome this difficulty by applying a mean field approximation to the threshold process in a novel manner. By doing so, we create differential equation models that capture the average performance of systems with probabilistic threshold dynamics.

Our approach is novel in that we incorporate the distribution of the threshold time, which may be dependent on the dynamic system state, to create a representation of the average value of the thresholded process. Our model produces a time-trace of the expected state of the system, as well as an explicitly time-dependent, cumulative distribution of the threshold time.

The advantages to be had are numerous. First, by creating a differential equation model, we are able to verify simulation models by comparing them against analytic results derived from the differential equations. Second, we may use the fast, cheap, differential equation model as a scoping tool to help us focus on areas of interest for complex, expensive simulations. Additionally, as a by-product, the model produces the time-dependent cumulative distribution of the threshold time, which prior to modeling may be expressed in terms of the dynamic system state and therefore may not have explicit time dependence. Finally, after developing the theory, we provide two worked examples, along with a step-by-step tutorial on how to apply this method to any thresholded system with a differential equation model.

The organization of the paper is as follows: In Section 2, we review the applicable literature. In Section 3, we derive our novel methodology through mean-field approximations of a cyber infection example, and extract the step-by-step procedure for applying it to other systems. In Section 4, we apply the step-by-step procedure to the Lanchester model of armed conflict. In Section 5, we provide numerical examples comparing the differential equation models to simulations. In Section 5, we also demonstrate that the differential equations from our novel methodology are fundamentally different from differential equations for a nonthresholded system; in other words, no choice of parameters of the nonthresholded differential equations may replicate the behavior of the thresholded differential equations. Finally, in Section 6, we provide some discussion of and directions for future research.

2 Literature Review

The general theory and application of differential equation models for physical and social phenomena is a common topic that spans several disciplines, including applied mathematics, biology, and operations research. Many good overviews of the topic exist; for a general text, we recommend *Differential Equation Models* by Braun (1983). For an overview of basic analysis and solution techniques, we recommend *Advanced Engineering Mathematics* (O'Neil, 1991).

The history and specific application differential equation models to epidemics is covered in detail in *Epidemic Modeling* (Daley & Gani, 1999) (see also Anderson & May [1979a, b]). For an accessible overview, we recommend the recent tutorial by Dimitorv and Meyers (2010). Specific applications of epidemics are addressed in the literature as well; fitting data is addressed by Mollision (1995), and stochastic epidemics are reviewed in detail by Andersson (2000). Specific system behaviors related to our research, such as time of discovery thresholds, are addressed by Metz, Wedel, and Angulo (1983). The distribution of the number of infected individuals at the moment of first detection is studied by Trapman, Christofel, and Bootsma (2009).

The application of infectious disease models to computer infections has been recommended by Project JASON (2010), an independent group of scientists advising the United States government. A related and noteworthy reference is the case study of the Code Red worm by Moore, Shannon, and Brown (2002).

The work most closely related to our model of cyber infections is Vojnovic and Ganesh (2005). Their model closely matches the dynamics of ours in that machines may be in two competing states—infected or patched—and the system operator wishes to maximize the number of patched machines. We extend their work by making the detection process an explicit function of the infection process.

Two recent books by Newman (2006, 2010) describe the formulation and analysis of network models and include cases of epidemics spread on networks as well as the general theory of mean-field approximations. Our work is different in that we consider both epidemic detection and spread simultaneously in a single, integrated framework.

Mean-field approximations are frequently used in physics; for an in-depth overview, see the second chapter of Freericks (2006). An overview of approximation methods for probabilistic methods is given by Darling and Norris (2008). Mean-fields have been applied in epidemic

models of network infections by Lelarge and Bolot (2008), and a development of their applicability to general infectious disease models is given in Kleczkowski and Grenfell (1999), who justify the use of the mean-field approximation for sufficiently large, nonhomogeneous networks.

For differential equation combat models, we recommend the original paper by Lanchester (1916). An historical application to the Battle of Iwo Jima appears in Engel (1954), and is further developed by Samz (1971). Comprehensive reviews of Differential equations models may be found in the books by Hartley (2001), and Washburn and Kress (2009). Of particular relevance a paper by Bracken appearing in Bracken, Kress, and Rosenthal (1995) applying Lanchester models to the Ardennes campaign. This formulation includes a threshold similar to the one we propose.

3 Modeling Sharp Thresholds

In this section, we describe a basic discrete-time, discrete-state system that models the spread of a cyber infection. We use mean-field approximations to derive our novel methodology of modeling the system using differential equations. Finally, in Section 3.4, we step back from the analysis of the cyber infection to pull out a generalized, step-by-step process for repeating the derivation in other systems.

3.1 Individual Discrete-Time Dynamics

We begin by considering a model of the spread of malicious code in a finite population of machines in discrete time. For ease of exposition, we use the term *virus* loosely to describe all malicious code that spreads via intramachine contact, to include worms, viruses, etc. Similarly, we use the term *infected* to mean that a machine currently has a virus somewhere in the machine.

We begin with a few basic definitions to facilitate the exposition. There is a fixed population of N machines. At any time, a machine may be in one of the following three states:

Class S: a machine is susceptible, in class S, if it is not currently infected, but may become infected if it interacts with an infected machine.

Class I : a machine is infected, in class I, if it is currently infected and may spread the infection by interaction with a machine of class S.

Class R : a machine is removed, in class R, if it is currently not infected and is immune to infection. A machine may join class R from either class S or I by having a patch installed.

As a preventative measure, a system administrator may specifically design or designate m machines as *sentinels*, which are machines that are monitored for infection. A virus may only be detected when it infects a sentinel. After detection, antivirus measures, which we collectively refer to as *patches*, may be developed and distributed.

Our model has three linked processes: predetection spread, detection, and postdetection spread. Next, we describe a discrete-time, discrete-state mathematical model of infection progression for each process individually.

3.1.1 Predetection Process

In this section, we describe the discrete-time, discrete-state infection process before detection occurs, which is a standard *S-I* model of infectious disease see (Daley & Gani, 1999). We denote the number of predetection infected machines in round t with I_t^P, and predetection susceptible machines in round t with S_t^P. Spread starts at $t = 0$ with I_0 infected machines and S_0 susceptible machines.

The predetection discrete-time infection process proceeds in rounds. During each round, each machine in class I^P selects a partner machine from the population, uniformly at random, for interaction. If the partner machine is of class I^P, no changes occur. If the partner machine is of class S^P, the partner machine transitions from S^P to I^P with probability β. The number of infected and susceptible machines in round t is random, and the evolution of $\left(S_t^P, I_t^P\right)$ forms a Markov chain. We can express the conditional expectation of each coordinate in round $t+1$ in terms of the coordinates in round t as:

$$\mathrm{E}\left[S_{t+1}^P \mid S_t^P, I_t^P\right] = S_t^P - \frac{\beta S_t^P I_t^P}{N} \tag{1}$$

$$\mathrm{E}\left[I_{t+1}^P \mid S_t^P, I_t^P\right] = I_t^P + \frac{\beta S_t^P I_t^P}{N}. \tag{2}$$

Equation (2) states that the expected number of infecteds in round $t+1$ is the number of infecteds in round t plus the expected number of newly created infecteds, $I_t^P \cdot S_t^P \cdot \frac{\beta}{N}$. Similar reasoning gives the first equation. The expectation expressions are an approximation, assuming large population size, N, I small relative to N, so that the likelihood of two infecteds choosing the same susceptible is negligible.

3.1.2 Postdetection Process

In this section, we describe the infection process after detection occurs, which is similar to the classic S-I-R model (see Daley & Gani, 1999). When detection occurs, a *patch* is distributed to all machines in the population: this is a piece of code that, if installed, removes any existing infection and makes the machine(s) resistant to any future infections. Each machine adopts the patch independently with probability μ in each round. We denote postdetection infecteds in round t by I_t^D, postdetection susceptibles in round t by S_t^D, and postdetection removeds in round t by R_t^D.

Postdetection dynamics begin immediately after detection occurs. When detection occurs, say in round t_*, members of the population who were infected remain infected; i.e., $I_{t_*}^D = I_{t_*}^P$. The

virus continues to spread with the same dynamics as predetection; i.e., the expected number of newly created infecteds in round $t+1$ is $\frac{\beta I_t^D S_t^D}{N}$. However, both susceptible machines and infected machines are removed with probability μ.

The random variables $\left(S_t^D, I_t^D, R_t^D\right)$ form a Markov chain in a manner similar to the $\left(S_t^P, I_t^P\right)$ variables. Assuming that detection has occurred in round $t_* \leq t$, the expectation of these random variables in round $t+1$ is:

$$\begin{aligned}
\mathrm{E}\left[S_{t+1}^D \mid S_t^D I_t^D R_t^D\right] &= S_t^D - \frac{\beta S_t^D I_t^D}{N} - \mu S_t^D \\
\mathrm{E}\left[I_{t+1}^D \mid S_t^D I_t^D R_t^D\right] &= I_t^D + \frac{\beta S_t^D I_t^D}{N} - \mu I_t^D \\
\mathrm{E}\left[R_{t+1}^D \mid S_t^D I_t^D R_t^D\right] &= R_t^D + \mu\left(I_t^D + S_t^D\right).
\end{aligned}$$

The above equations are nearly identical to the classic S-I-R model, except that they include transitions directly from S to R by patch installation. Because they are difference equations, the rates β and μ are assumed to be less than one; this is a restriction that will be lifted when moving to continuous time.

3.1.3 The Detection Process

We are now ready to consider the detection process probabilistically, which is our main contribution. During each round, the m sentinels have the opportunity to contract and detect the virus. We assume that the m sentinels are reselected in a uniform random manner from the population of N machines in each round; this simplifies the model by removing the necessity to track the number of infected sentinels. Detection at an infected sentinel occurs probabilistically. Let α be the probability that a single infected sentinel does not detect the infection in a single time period. This choice of parameterization will prove useful in the following development. Let D_t be an indicator random variable of the detection event:

$$D_t = \begin{cases} 1 & \text{if detection has occurred by time } t \\ 0 & \text{otherwise.} \end{cases}$$

Consider the sequence of differences, $D_t - D_{t-1}$. Members of this sequence are equal to zero

everywhere, except in the round of detection. For the round of detection, when t equals t_*, the difference is equal to one. We may write the expectation of this difference as

$$\begin{aligned}\mathrm{E}[D_t - D_{t-1}] = \Pr[D_{t-1} = 0] \cdot \mathrm{E}\left[D_t - D_{t-1} \mid D_{t-1} = 0\right] \\ + \Pr[D_{t-1} = 1] \cdot \mathrm{E}\left[D_t - D_{t-1} \mid D_{t-1} = 1\right].\end{aligned} \tag{3}$$

The second term in Equation (3) is equal to zero because if detection occurred by round $t-1$, it has also occurred by round t. Because the difference expression is nonzero only if detection occurs in round t, we can rewrite the first term in the expression as

$$\Pr[D_{t-1} = 0] \cdot \mathrm{E}\left[D_t - D_{t-1} \mid D_{t-1} = 0\right] = \Pr[D_t = 1, D_{t-1} = 0]. \tag{4}$$

The right-hand side of Equation (4) expresses the probability that detection occurs on round t and has not occurred in rounds 1 through $t-1$. Given I_i^P, the probability that detection occurs in round i is $1 - \alpha^{\frac{I_i^P m}{N}}$, where the exponent comes from computing the expected number of infected sentinel machines if sentinel machines are chosen uniformly from the population. Let $I_{t:0}^P$ denote the sequence $I_t^P, \ldots, I_0^P$. From Equations (3) and (4), we have

$$\mathrm{E}[D_{t+1} - D_t \mid I_{t:0}^P] = \left(1 - \alpha^{\frac{I_t^P m}{N}}\right) \prod_{k=0}^{t-1} \alpha^{\frac{I_k^P m}{N}}, \tag{5}$$

which is the fundamental difference equation for the D process in this example.

3.2 Coupling the Postdetection and Predetection Processes

The key to properly modeling the sharp change in infection dynamics is the coupling of the predetection process and the postdetection process, as governed by the random detection process. In particular, in the round of detection, it is necessary to move all machines from the predetection dynamics to the new postdetection dynamics. For a graphical depiction of coupling, see Figure 1.

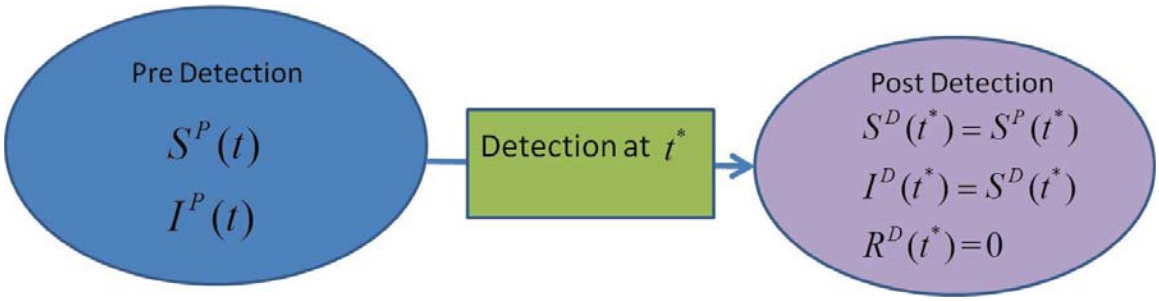


Figure 1: Depiction of Coupling. In the round of detection, which we call t^*, the state of the predetection process is transferred to the postdetection process.

Let (S_t, I_t) be a Markov chain that evolves as an undetected predetection process for all t. Using the notation in the previous sections for predetection and postdetection machines, we can then write the coupled predetection process as

$$\begin{aligned} S_t^P &= (1 - D_t)S_t \\ I_t^P &= (1 - D_t)I_t. \end{aligned}$$

Intuitively, the above expressions say that before detection has occurred—when D_t is 0—the predetection process evolves as specified in Section 3.1.1; and after detection has occurred—when D_t is 1—there are no machines in the S^P and I^P classes. For brevity, let

$$\overline{A}_t = (S_t, I_t, S_t^P, I_t^P, D_t, D_{t-1}, S_t^D, I_t^D, R_t^D)$$

denote the state of a Markov chain describing evolution of the cyber infection. We can write the evolution of the coupled postdetection process as

$$\begin{aligned} \mathrm{E}\left[S_{t+1}^D \mid \overline{A}_t\right] &= (D_t - D_{t-1})S_t + S_t^D - \frac{\beta S_t^D I_t^D}{N} - \mu S_t^D \\ \mathrm{E}\left[I_{t+1}^D \mid \overline{A}_t\right] &= (D_t - D_{t-1})I_t + I_t^D + \frac{\beta S_t^D I_t^D}{N} - \mu I_t^D \\ \mathrm{E}\left[R_{t+1}^D \mid \overline{A}_t\right] &= R_t^D + \mu\left(I_t^D + S_t^D\right). \end{aligned}$$

Intuitively, the above expressions say that in the round when detection occurs—the only time that $D_t - D_{t-1}$ is 1—a sudden inflow of of machines, equal to the machines in the undetected I and S classes, comes into the postdetection classes. Afterward, the postdetection classes behave as described in Section 3.1.2. This allows us to write the discrete time difference equations for

all of the variables involved as

$$\mathrm{E}\left[S_{t+1} \mid \overline{A}_t\right] - S_t = -\frac{\beta S_t I_t}{N} \tag{6a}$$

$$\mathrm{E}\left[I_{t+1} \mid \overline{A}_t\right] - I_t = \frac{\beta S_t I_t}{N} \tag{6b}$$

$$\mathrm{E}[D_{t+1} \mid I^P_{t:0}] - \mathrm{E}[D_t \mid I^P_{t:0}] = \left(1 - \alpha^{\frac{I^P_t m}{N}}\right) \prod_{k=0}^{t-1} \alpha^{\frac{I^P_k m}{N}} \tag{6c}$$

$$S^P_t = (1 - D_t) S_t \tag{6d}$$

$$I^P_t = (1 - D_t) I_t \tag{6e}$$

$$\mathrm{E}\left[S^D_{t+1} \mid \overline{A}_t\right] - S^D_t = (D_t - D_{t-1}) S_t - \frac{\beta S^D_t I^D_t}{N} - \mu S^D_t \tag{6f}$$

$$\mathrm{E}\left[I^D_{t+1} \mid \overline{A}_t\right] - I^D_t = (D_t - D_{t-1}) I_t + \frac{\beta S^D_t I^D_t}{N} - \mu I^D_t \tag{6g}$$

$$\mathrm{E}\left[R^D_{t+1} \mid \overline{A}_t\right] - R^D_t = \mu \left(I^D_t + S^D_t\right). \tag{6h}$$

Intuitively, the superscript in the difference equation for D is I^P instead of I because the difference $\mathrm{E}[D_{t+1} \mid I^P_{t:0}] - \mathrm{E}[D_t \mid I^P_{t:0}]$ is zero after detection occurs. As written, indeed, after detection occurs, I^P is zero, and the difference $\mathrm{E}[D_{t+1} \mid I^P_{t:0}] - \mathrm{E}[D_t \mid I^P_{t:0}]$ is zero. If I were used instead, the difference would never be zero because the I process is not affected by detection, and asymptotically approaches the total population as t increases.

3.3 Moving to Continuous Time

To move to continuous time from the unit time, discrete difference equations, (6a)–(6h), we create a sequence of random processes, each moving at a smaller and smaller time interval, Δt. In each of these processes, we scale the parameters β, μ, and α so as to keep the expected number of events per unit time constant.

The parameter β gives the expected number of infections per unit time. For a process that proceeds in time intervals of Δt, the parameter should be scaled to $\Delta t \beta$ because the faster-moving process has $\frac{1}{\Delta t}$ attempts at infection per unit time. Similar reasoning shows that the parameter μ should be scaled to $\Delta t \mu$.

The correct scaling for the parameter α is more delicate. In the unit time progression process, a single infected sentinel does not detect the infection with probability α in each round. The scaling of the parameter should be such that the probability an infected sentinel does not detect

the infection remains α for a unit of time. Let α_Δ denote the scaled parameter. The property we seek is $\alpha_\Delta^{\frac{1}{\Delta t}} = \alpha$, because in the faster-moving process, an infected sentinel has $\frac{1}{\Delta t}$ attempts at detection. Preserving the desired property gives us a scaling of $\alpha_\Delta = e^{\Delta t \ln(\alpha)}$.

The next step of the derivation involves the mean-field assumption, which equates a random variable and its expectation. In general, this step is controversial because it is a heuristic argument, in the sense that it is not explicitly predicated on taking limits of random processes using tools like the functional central limit theorem (Billingsley, 1968). On the other hand, it is possible to rigorously derive convergence results based on these heuristic approaches, at the cost of a significant increase in mathematical complexity (McNeil, 1973). It is even possible to derive results on the variance of the stochastic process from the means described by the differential equations (Barbour, 1974). Practically, many researchers jump directly to the differential equation models, without considering the underlying Markov chain at all (Keeling, 2007; Newman, 2010). For our purposes, we choose to be explicit in the heuristic limiting argument, without predication on functional central limit theorem, and numerically check the accuracy of the resulting differential equation against a simulation of the Markov chain in Section 5.

With the appropriately scaled parameters, we can begin with the discrete time difference equations for a process moving in time steps of Δt, apply the mean-field assumption equating a random variable and its expectation, and take the limit as Δt approaches zero to derive the continuous time differential equations. We can follow these steps for each of the Equations (6a)–(6h), but for exposition we give a few examples highlighting the important details.

For Equation (6a), the process moving at Δt time intervals has the equation

$$\mathrm{E}\left[S_{t+\Delta t} \mid \overline{A}_t\right] - S_t = -\frac{\Delta t \beta S_t I_t}{N}.$$

Applying the mean-field assumption, and dividing both sides by Δt, we have

$$\frac{S_{t+\Delta t} - S_t}{\Delta t} = -\frac{\beta S_t I_t}{N}.$$

Taking the limit of both sides as Δt goes to zero, we have

$$\frac{dS(t)}{dt} = -\frac{\beta S(t) I(t)}{N},$$

which is the final continuous time equation for the S class. The equation for the I class can be derived similarly.

Deriving the continuous time equation for D is slightly more involved, but consists of the same set of steps. First, we begin with the difference equation for a process moving at Δt time intervals,

$$\mathrm{E}[D_{t+\Delta t} \mid I^P_{t:0}] - \mathrm{E}[D_t \mid I^P_{t:0}] = \left(1 - e^{\Delta t \ln(\alpha) \frac{I^P_t m}{N}}\right) \prod_{k=0}^{t-1} e^{\Delta t \ln(\alpha) \frac{I^P_k m}{N}}.$$

Applying mean-field, dividing both sides by Δt, and taking the limit as Δt approaches zero, we have

$$\lim_{\Delta t \to 0} \frac{D_{t+\Delta t} - D_t}{\Delta t} = \lim_{\Delta t \to 0} \frac{\left(1 - e^{\Delta t \ln(\alpha) \frac{I^P_t m}{N}}\right) e^{\Delta t \ln(\alpha) \frac{m}{N} \sum_{k=0}^{t-1} I^P_k}}{\Delta t}.$$

We apply L'Hopital's rule on the right-hand side to derive

$$\begin{aligned}
\frac{dD(t)}{dt} = \lim_{\Delta t \to 0} \Bigg[& -\ln(\alpha) \frac{I^P_t m}{N} e^{\Delta t \ln(\alpha) \frac{m}{N} \sum_{k=0}^{t} I^P_k} \\
& + \left(1 - e^{\Delta t \ln(\alpha) \frac{I^P_t m}{N}}\right) e^{\Delta t \ln(\alpha) \frac{m}{N} \sum_{k=0}^{t-1} I^P_k} \left(\ln(\alpha) \frac{m}{N} \sum_{k=0}^{t-1} I^P_k\right) \Bigg] \\
= & -\ln(\alpha) \frac{I^P_t m}{N},
\end{aligned}$$

which gives the final continuous time equation for the D variable.

To finish deriving the continuous time system, Equations (6d) and (6e) directly translate into their continuous time equivalents.

$$\begin{aligned}
S^P(t) &= (1 - D(t)) S(t) \\
I^P(t) &= (1 - D(t)) I(t).
\end{aligned}$$

However, for the purposes of a uniform presentation, it may be desirable to represent these as

differential equations, which, by the chain rule are:

$$\frac{dS^P(t)}{dt} = -\frac{dD(t)}{dt}S(t) + (1 - D(t))\frac{dS(t)}{dt}$$
$$\frac{dI^P(t)}{dt} = -\frac{dD(t)}{dt}I(t) + (1 - D(t))\frac{dI(t)}{dt}.$$

Finally, Equations (6f)–(6h) can be converted into continuous equivalents through the standard route of applying the mean-field approximation and taking limits to derive the complete continuous system of equations for the sharp threshold process:

$$\frac{dS}{dt} = -\frac{\beta SI}{N} \tag{7a}$$
$$\frac{dI}{dt} = \frac{\beta SI}{N} \tag{7b}$$
$$\frac{dD}{dt} = -\ln(\alpha)\frac{I^P m}{N} \tag{7c}$$
$$\frac{dS^P}{dt} = -\frac{dD}{dt}S + (1 - D)\frac{dS}{dt} \tag{7d}$$
$$\frac{dI^P}{dt} = -\frac{dD}{dt}I + (1 - D)\frac{dI}{dt} \tag{7e}$$
$$\frac{dS^D}{dt} = \frac{dD}{dt}S - \frac{\beta S^D I^D}{N} - \mu S^D \tag{7f}$$
$$\frac{dI^D}{dt} = \frac{dD}{dt}I + \frac{\beta S^D I^D}{N} - \mu I^D \tag{7g}$$
$$\frac{dR^D}{dt} = \mu\left(I^D + S^D\right), \tag{7h}$$

where we have dropped the explicit dependence on t for brevity. The initial conditions for these equations place the starting number of infected machines in $I(0)$ and $I^P(0)$, the starting number of susceptible machines in $S(0)$ and $S^P(0)$, and set the start of all other variables to zero.

3.4 Discussion

To gain some understanding of Equations (7a)–(7h), we discuss their intuitive interpretation and the general steps to rederive them for different sharp-threshold random processes.

Equations (7a) and (7b) are tracking a prethreshold process as though the random threshold will never occur. Equation (7c) and the variable D provide a probability distribution for the threshold time. Specifically, $D(t)$ represents the cumulative distribution function of the random threshold time. The value of $\frac{dD}{dt}$ can be interpreted simply as the probability density function of the random threshold. For this particular example, $D(t)$ posesses a closed-form solution (see Appendix B).

Equations (7d) and (7e) capture the expected random process trajectories that remain prethreshold. This can be seen in two ways, first by considering the equations $S^P = (1 - D)S$ and $I^P = (1 - D)I$. The factor $(1 - D)$ represents the probability that threshold has not occurred, and only those trajectories where threshold has not occurred stay in the prethreshold classes. The corresponding derivatives in Equations (7d) and (7e) also have natural interpretations. The first term subtracts any trajectories where threshold instantaneously occurs. The second term dampens the rate of change, making sure it is proportional to the trajectories where threshold has not occurred.

Equations (7f)-(7h) capture the random process trajectories that are postthreshold. The first term in Equations (7f) and (7g) captures the instantaneous inflow of new trajectories, while the second term computes the change for the postthreshold dynamics. There is no direct inflow of prethreshold trajectories into the R^D class, so it does not have a term with $\frac{dD}{dt}$. Also, there is no need to dampen the postthreshold changes, the second and third terms of (7f) and (7g), as they are naturally dampened by the fact that only the trajectories that inflow postthreshold are used to compute postthreshold changes. The general steps to derive similar sharp threshold equations for other systems are the following:

1. Write down an unencumbered prethreshold system of equations. This is the equivalent of Equations (7a) and (7b), and variables S and I.

2. Define a variable D to describe the cumulative distribution function of threshold time. Its differential equation with respect to time is the probability density function for the threshold time. This is the equivalent of Equation (7c). This probability density function may depend on both t and the expected prethreshold variables, the equivalent of S^P and I^P.

3. Set the expected prethreshold variables to be $(1 - D)$ times the unencumbered prethreshold variables. This also defines differential equations of the expected prethreshold vari-

ables with respect to t. This is the equivalent of Equations (7d) and (7e).

4. Write a postthreshold system of equations. Add terms of $\frac{dD}{dt}$ times the unencumbered variables for direct inflow due to threshold occurrence. This is the equivalent of Equations (7f)–(7h).

As we demonstrate computationally in Section 5, these steps are necessary to correctly track sharp threshold dynamics. Without a similar approach, as adding the unencumbered system and the D variable, there is insufficient state memory to capture sharp threshold dynamics, and we see inaccuracies in the deterministic predictions versus the expected state of the underlying random process.

4 Application to Lanchester Equations

In this section, we employ steps 1-4 from the previous section to develop a novel thresholded model of combat based on Lanchester's equations. This is important both in its own right as a contribution to combat models, as well as an example of steps 1-4 in Section 3.4.

Our mathematical model concerns cases where there is an immediate, global loss of effectiveness for one of the combatants. Such a loss of effectiveness stems from the loss of a key capability, such as a communication network or vital asset, and could be the result of adversary action or other failure.

Lanchester's original model involves two opposing teams: the blue forces and the red forces. The total amount of blue forces available at time t is denoted by the variable $B(t)$, and the total amount of red forces available at time t is denoted by the variable $R(t)$. Lanchester's original *aimed fire* equations assume that each red unit has a likelihood of ρ of removing a blue unit, while each blue unit has a likelyhood of β of removing a red unit. Lanchester describes the evolution of the battle as:

$$\frac{dB(t)}{dt} = -\rho R(t) \tag{8a}$$

$$\frac{dR(t)}{dt} = -\beta B(t), \tag{8b}$$

where ρ, β are effectiveness parameters of the red (blue) sides, respectively. These equations have been well studied and applied to numerous case studies (see Washburn & Kress, 2009). We seek to generalize Lanchester's equations to consider cases where one of the effectiveness parameters, say β is suddenly and irrevocably reduced its prethreshold value to a lower, post-threshold value, say β^-. This models the loss of a key capability for the blue forces. To create the threshold model of the Lanchester equations, we follow steps 1-4 outlined in Section 3.4.

1. We write the unencumbered prethreshold system of equations. In this case, they are identical to Lanchester's original formulation as shown in Equations (8).

2. We define a variable $D(t)$, that describes the cumulative distribution function of threshold time. For this example, we choose an exponentially distributed threshold time, with rate parameter λ. This gives $\frac{dD(t)}{dt} = \lambda e^{-\lambda t}$, the probability density function, and $D(t) = 1 - e^{-\lambda t}$, the cumulative distributed function, with $D(0) = 0$.

3. We now write the prethreshold equations, dropping the dependence on t for brevity,

$$\frac{dB^P}{dt} = -\frac{dD}{dt}B + (1-D)\frac{dB}{dt}$$
$$\frac{dR^P}{dt} = -\frac{dD}{dt}R + (1-D)\frac{dR}{dt}.$$

Similarly to the cyber infection example, these equations result from setting $B^P = (1-D)B$ and differentiating.

4. We now write the postthreshold equations, adding terms of $\frac{dD}{dt}$, which model inflow, where appropriate:

$$\frac{dB^D}{dt} = \frac{dD}{dt}B - \rho R^D$$
$$\frac{dR^D}{dt} = \frac{dD}{dt}R - \beta^- B^D.$$

The four steps generate the complete set of differential equations

$$\frac{dB}{dt} = -\rho R \tag{9a}$$
$$\frac{dR}{dt} = -\beta B \tag{9b}$$
$$\frac{dD}{dt} = \lambda e^{-\lambda t} \tag{9c}$$
$$\frac{dB^P}{dt} = -\frac{dD}{dt}B + (1-D)\frac{dB}{dt} \tag{9d}$$
$$\frac{dR^P}{dt} = -\frac{dD}{dt}R + (1-D)\frac{dR}{dt} \tag{9e}$$
$$\frac{dB^D}{dt} = \frac{dD}{dt}B - \rho R^D \tag{9f}$$
$$\frac{dR^D}{dt} = \frac{dD}{dt}R - \beta^- B^D. \tag{9g}$$

The model can be initialized by $B(0)$ and $B^P(0)$ to the initial blue forces, setting $R(0)$ and $R^P(0)$ to the initial red forces, and all other variables to zero.

5 Numerical Analysis

In this section, we compare our theoretical results with simulations to verify that the differential equations do indeed track the average state of the underlying Markov chain. This is a critical step in verifying the differential equation models because mean-field approximations assume equality between a random variable and its mean—and thus provide no mathematical guarantee on the result. We do this numerical analysis and verification for both the cyber infection model developed in Section 3 and the Lanchester model of Section 4. We also demonstrate that the models we develop are fundamentally different than the original systems of differential equations by showing that no parameterization of the original differential equations yields correct behavior.

Figure 2 depicts a comparison of a simulation of cyber infection to thresholded model as presented in Equations (7). Both the simulation and the differential equations use a parameterization of $(\beta, \alpha, m, N, \mu) = (0.01; 0.99; 20; 100,000; 0.2)$ and 100 initially infected machines. The dashed lines indicate the average state of $2,000$ simulation runs; i.e., the average state of the Markov chain at time t, for each of the predetection and postdetection classes. The solid lines with markers indicate the numerical integration of the differential equations. For all pre and postdetection classes, the average of the simulation runs agrees with the differential equations. Our choice of parameterization, in particular $\mu = 0.2$, results in highly variable postdetection classes, S^D and I^D. This variance is a result of the quick adoption of the patch after detection has occurred. The plots of S^D and I^D indicate a benefit of the differential equations—that they can produce the mean state of the system without the requirement for thousands of simulations. In addition, Figure 2 depicts agreement between the empirical distribution of detection time, derived from the simulation and pictured as a histogram, versus the variable D in the differential equation system. This demonstrates another benefit to the differential equation system: the differential equation system can produce a distribution of threshold time even when the threshold time is a function of the system state, as is the case for the cyber infection model.

The model described by Equations (7) split pre and postdetection susceptibles and infecteds into different classes; however, an analyst may be interested simply in the number of susceptibles and infecteds at time t. Figure 3 depicts a comparison between simulation and differential equations on the number of susceptibles at time t, $S^P + S^D$, and the number of infecteds at time t, $I^P + I^D$. The dashed lines indicate the average state of 2,000 simulation runs, and the solid marked lines indicate the result of the differential equations. In addition, the figure includes a

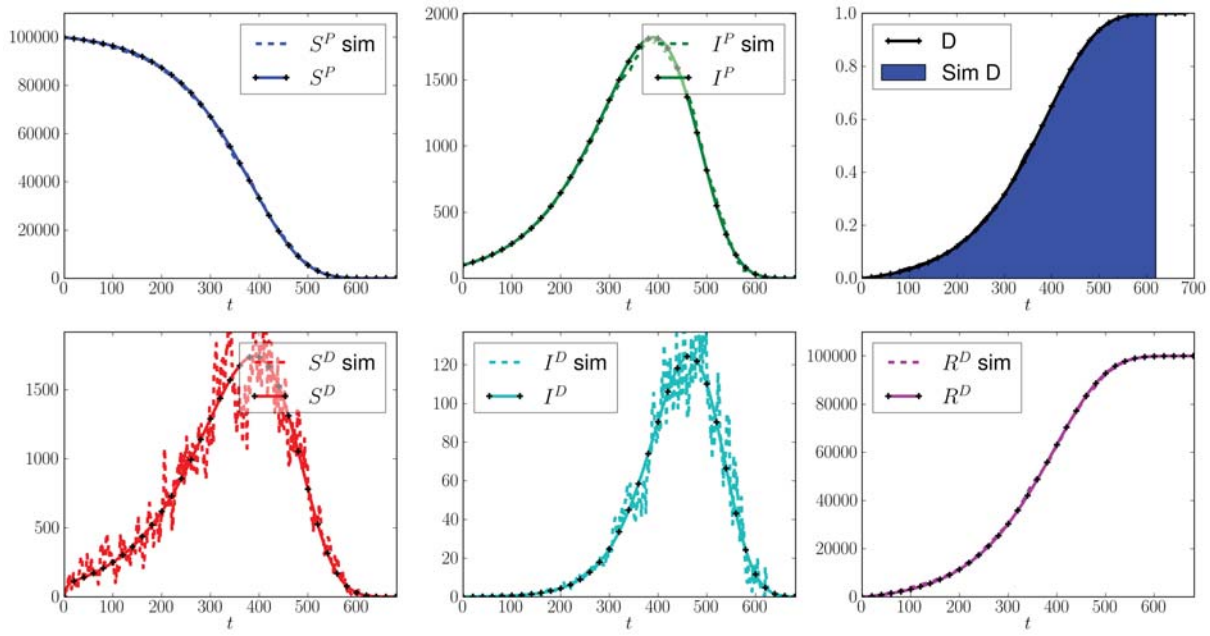
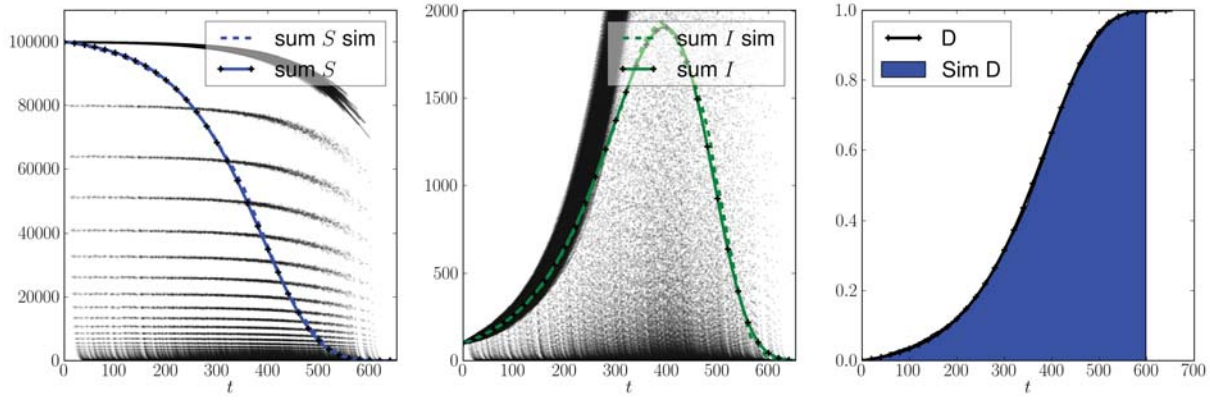


Figure 2: Cyber infection model simulation versus differential equations. Both methods use a parameterization of $(\beta, \alpha, m, N, \mu) = (0.01; 0.99; 20; 100,000; 0.2)$ and 100 initially infected machines. The dashed lines indicate the average state of $2,000$ simulation runs, and the solid lines with markers indicate the numerical integration of the differential equations. The parameter $\mu = 0.2$ models quick adoption of the patch and results in variable postdetection classes, S^D and I^D. The differential equations produce the mean state of the system accurately, even with this variance. The top right graph depicts agreement between the empirical distribution of detection time, derived from the simulation and pictured as a histogram, versus the variable D in the differential equation system. In this process, the detection time is a function of the system state.



[h!]

Figure 3: Total susceptibles and infecteds in cyber infection model. The dashed lines indicate the average state of $2,000$ simulation runs, and the solid marked lines indicate the result of the differential equations, $S^P + S^D$ and $I^P + I^D$. The black dots depict a scatter plot of the state of the $2,000$ simulations. The models use the same parameterization as in Figure 2. The striations in the scatter plot for susceptibles is due to the fast adoption of the patch, $\mu = 0.2$. Approximately 20% of machines adopt the patch in each round. The differential equation system accurately captures the average state of the system.

scatter plot for the 2,000 runs. The variance due to the fast adoption of the patch, $\mu = 0.2$, is evident in the bands in the scatter plot for susceptibles. Once detection occurs, approximately 20% of machines adopt the patch in each round, resulting in the striation in the figure. Even with this large amount of variance in the individual simulation runs, the differential equation system accurately captures the average state of the system.

Figure 4 depicts a comparison of a Lanchester combat model simulation to the corresponding differential equation model as presented in Equations (9). Both the simulations and the differential equations use a parameterization $(\rho, \beta, \beta^-, \lambda) = (0.01, 0.02, 0.001, \frac{1}{25})$ and initial sizes of 100,000 for both the blue and red forces. The differential equations agree with the mean state of the system, except at higher values of t. This disagreement is due to the well-known inaccuracy of the standard Lanchester aimed fire model as presented in Equations 8 (8) (see Washburn & Kress, [2009] and Taylor, [1983]). The standard Lanchester model is inaccurate because it overestimates the effectiveness of a large force against a small force, possibly even resulting in negative force sizes. The inaccuracy in the standard Lanchester model, which is beyond the scope of this work, gives the disagreement between the simulations and the differential equations for the class B^D at high values of t. For small values t, less than approximately 120 in the figure, the average state of the simulations agrees with the differential equations.

Figure 5 depicts the expected size of the blue and red forces at time t. The dashed lines depict the average of $2,000$ simulations, while the solid marked lines depict the sums $B^P + B^D$ and $R^P + R^D$. The figure also includes a scatter plot of the states of the 2,000 simulation runs. The striations in the scatter plot for the red forces is due to variance in the threshold time. Before the threshold, the blue forces are highly effective against red, and after the threshold they become ineffective. For an individual simulation, the red forces would follow the sharp down curve, until threshold time, at which point they would follow one of the flatter striations. Even with the highly variable force sizes between individual simulations, Equations (9) accurately captures the expected force sizes at time t.

Finally, Figure 6 demonstrates that our modeling method is fundamentally different than a simple application of previously existing models. Specifically, consider the Lanchester threshold system, where the sharp threshold simply reduces the effectiveness of the blue forces from β to β^-. One modeling approach may be to simply replace the parameter β in the standard Lanchester mode,l as presented in Equation (8), with an expected effectiveness parameter of the blue forces. In Figure 6, the solid lines represent the expected size of the red and blue forces under

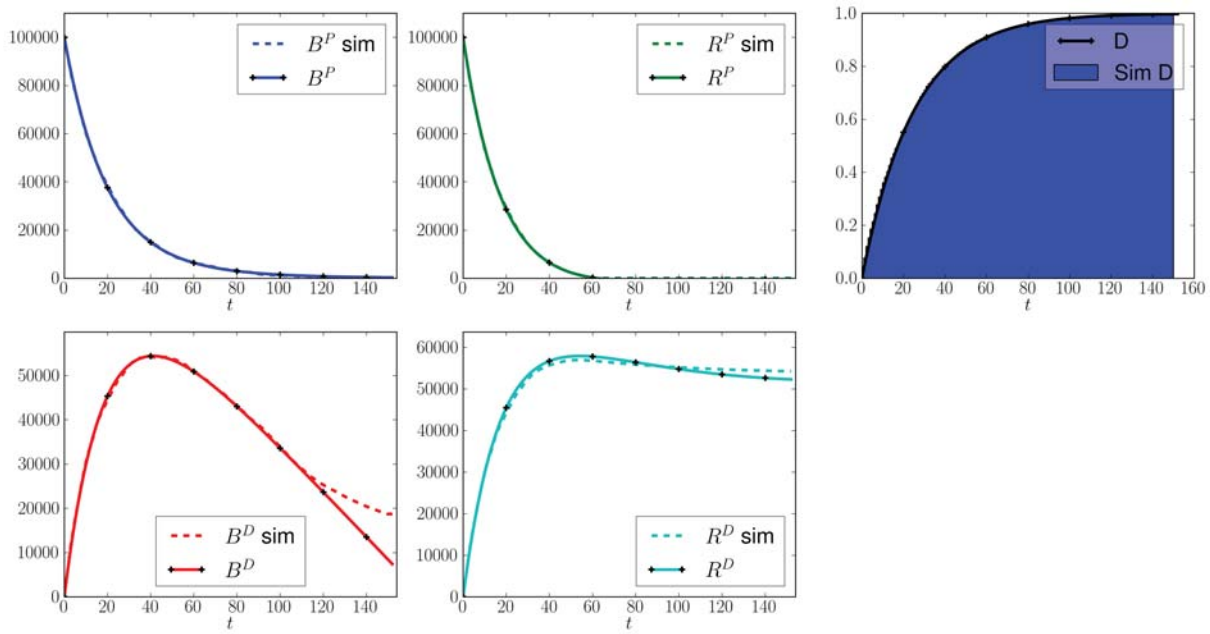


Figure 4: Lanchester combat model simulation versus differential equations. Both methods use a parameterization $(\rho, \beta, \beta^-, \lambda) = (0.01, 0.02, 0.001, \frac{1}{25})$ and initial sizes of 100,000 for both forces. The standard Lanchester model has inaccuracies at high values of t that give the disagreement between the simulations and the differential equations for the class B^D at high values of t. For small values t, less than approximately 120 in the figure, the average state of the simulations agrees with the differential equations.

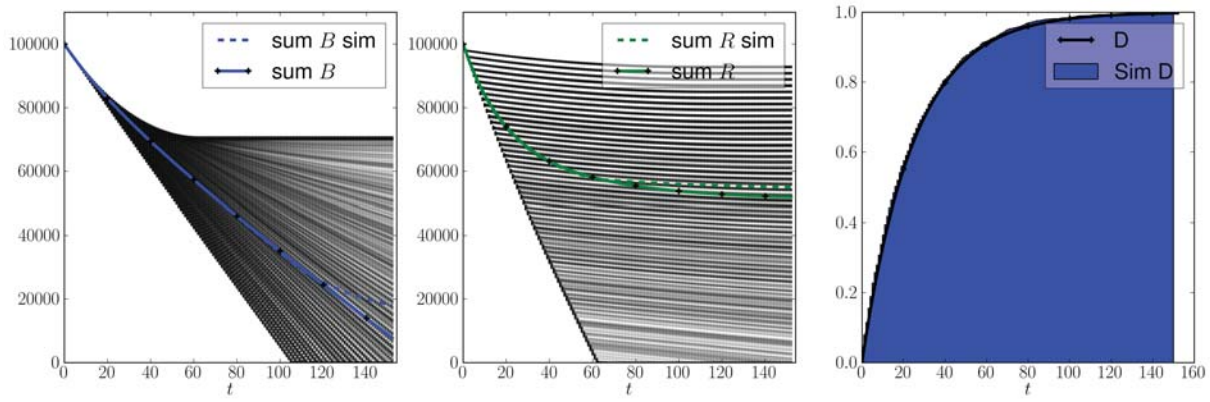


Figure 5: Total force sizes in Lanchester combat model. The dashed lines depict the average of 2,000 simulations, while the solid marked lines depict the sums $B^P + B^D$ and $R^P + R^D$. The scatter plot depicts states of the 2,000 simulation runs. The models use the same parameterization as Figure 4. For an individual simulation, the red forces follow the sharp down curve, until threshold time, at which point they follow one of the flatter striations. Even with the highly variable force sizes between individual simulations, Equation (9) accurately captures the expected force sizes at time t.

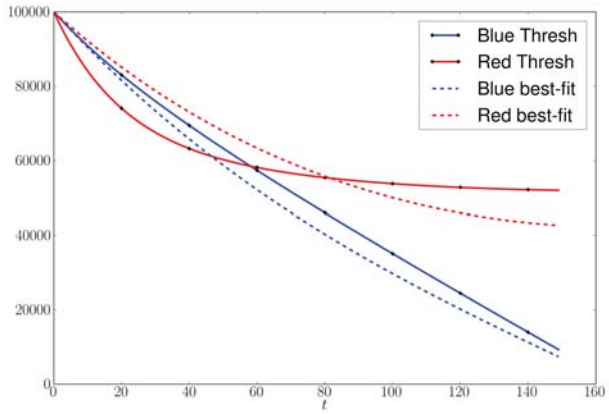


Figure 6: Best fit of a standard Lanchester model to a sharp threshold Lanchester model. The solid lines represent the expected size of the red and blue forces under Equation (9), while the dashed lines represent the closest fitting parameterization of Equation (8), a standard Lanchester model. The best fit optimization finds the parameter β for the standard Lanchester model that minimizes the squared error between the model's force sizes and Equationl (9)'s force sizes. All other parameters for both models are the same as those in Figure 4. The fit between the closest Lanchester model and our modeling method is poor, demonstrating that the sharp threshold models yield fundamentally new behavior. For this example, the red forces initially diminish rapidly, but after the sharp threshold, overwhelm the blue forces.

the model presented in Equations (9), while the dashed lines represent the closest fitting standard Lanchester model (see Equations [8]). The best fit standard Lanchester model results from a least-squares optimization on the parameter β, attempting to minimize the difference from the force sizes given by the model in Equations (9). The fit between the closest Lanchester model and our modeling method is poor. Our modeling approach yields fundamentally new behavior in that the red forces initially diminish rapidly, but after the sharp threshold, overwhelm the blue forces. Appendix A demonstrates that a naive approach—one which does not include the unencumbered system required by Step 1 in Section 3.4—to modeling the more complex problem of cyber infections also does not work.

6 Conclusions and Future Research

We extend the utility of differential equation models by incorporating the novel ability to model a probabilistic sharp threshold in system dynamics. We demonstrate our results with two applications: modeling cyber infections and capability loss in combat—both of which are of interest in their own right. For example, we hope that our cyber infection model will be useful in determining the relative merits of investment in additional detectors versus more rapid patch dissemination. Similarly, we hope that our Lanchester extension will be useful in quantifying the uncertainties and concerns inherent in unreliable, but powerful, capabilities. Beyond these two applications, we develop a simple, step-by-step procedure to model sharp thresholds in other systems. The steps described in Section 3.4 provide intuition and allow other modelers to create probabilistic sharp threshold models, without re-creating the steps in Section 3.

Future areas of study, based on our results, include: (1) to consider a broader set of problems against which to apply our novel modeling method; (2) to consider cases with multiple thresholds; e.g., the probabilistic loss of capabilities on both sides of the Lanchester model, or the restoration of a lost capability; and (3) to use the differential equations to describe the variance in the underlying Markov chain; the large amount of variance is visible in the numerical analysis for both examples we consider, and it would be interesting and relevant to describe that variance by perhaps using stochastic diffusion approaches.

References

[1] Andersson, H. (2000). *Stochastic epidemic models and their statistical analysis.* New York: Springer.

[2] Barbour, A. (1976). Quasi stationary distributions in Markov population processes. *Advances in applied probability. 8*,296–314.

[3] Billingsley, P. (1968). Convergence in probability measures. New York: Wiley.

[4] Bracken, J., Kress, M., & Rosenthal, R. (1995). *Warfare modeling.* Military Operations Research Society.

[5] Braun, M. (1983). *Differential equation models.* New York: Springer.

[6] Daley, D., & Gani, G. (1999). *Epidemic modeling: An introduction.* Cambridge: Cambridge University Press.

[7] Darling, R., & Norris, J. (2008). Differential equation approximations for Markov chains. *Probability surveys*. *5*,378–79.

[8] Dimitrov, N. B., & Meyers, L. A. (2010, November). Mathematical approaches to infectious disease prediction and control. *TutORials in Operations Research.* Hanover, MD: INFORMS.

[9] Engel, J. (1954). A verification of Lanchester's law. *Journal of the Military Operations Research Society of America*. *2*, 163–171.

[10] Freericks, J. (2006). *Transport in multilayered nanostructures: The dynamical mean-field theory approach*. London: Imperial College Press.

[11] JASON. (2010). The science of cyber-security. Washington, D.C.: The MITRE Corporation.

[12] Keeling, M., & Rohani, P. (2007). *Modeling infectious diseases in humans and animals.* Princeton, NJ: Princeton University Press.

[13] Kleczkowski, A., & Grenfell, B. (1999). Mean field type of equations for the spread of epidemics: The small world model. *Physica A*. *274*, 355–360.

[14] Lanchester, F. (1916). *Aircraft in warfare: The dawn of the fourth arm*. New York: Appleton.

[15] Lelarge, M., & Bolot, J. (2008). A local mean field analysis of security investments in networks. In *Proceedings of the 3rd international workshop on economics of networked systems*, NetEcon '08.

[16] McNeil, D., & Schach, S. (1973). Central limit analogues for Markov population processes. *Journal of the Royal Statistical Society, Series B. 35*, 1–23.

[17] Metz, J., Wedel, M., & Angulo, A. (1985). Discovering an epidemic before it has reaches a certain level of prevalence. *Biometrics. 39*, 765–770.

[18] Mollison, D. (1995). *Epidemic models: Their structure and relation to data*. Cambridge: Cambridge University Press.

[19] Moore, D., Shannon, C., & Brown, J. (2002). Code-Red: A case study on the spread and victims of an internet worm. *IN Proceedings of the 2nd ACM internet measurement workshop*, 273–284.

[20] Newman, M. (2006) *The structure and dynamics of networks.* Princeton, NJ: Princeton University Press.

[21] Newman, M. (2010) *Networks: An introduction*. Oxford: Oxford University Press.

[22] O'Neil, P. (1991). *Advanced engineering mathematics.* Bellmont CA: Wadsworth Publishing.

[23] Samz, R. (1971) Some comments on Engel's "A verification of Lanchester's law." *Operations Research. 20*, 49–52.

[24] Taylor, J. (1983). *Lanchester models of warfare, Volume I and II.* INFORMS, Arlington, VA.

[25] Trapman, P., Christoffel, M., & Bootsma, J. (2009). A useful relationship between epidemiology and queuing theory: The distribution of the number of infectives at the moment of first detection. *Math Biosci. 219*, 15–22.

[26] Vojnovic, M., & Ganesh, A. (2005). On the race of worms, alerts and patches. *ACM-SIGSAC Worm '05*.

[27] Washburn, A., & Kress, M. (2009). *Combat modeling*. New York: Springer.

A Naive Model for Cyber Infections

A naive approach to modeling the probabilistic sharp threshold for cyber infections ignores the unencumbered variables described in step 1 in Section 3.4. The naive approach results in the following system of equations:

$$\frac{d\hat{S^P}}{dt} = -\frac{\beta \hat{S^P} \hat{I^P}}{N} + \frac{\ln(\alpha) \hat{S^P} \hat{I^P} m}{N} \tag{A.1}$$

$$\frac{d\hat{I^P}}{dt} = \frac{\beta \hat{S^P} \hat{I^P}}{N} + \frac{\ln(\alpha) \hat{I^P} \hat{I^P} m}{N} \tag{A.2}$$

$$\frac{d\hat{S^D}}{dt} = -\frac{\ln(\alpha) \hat{S^P} \hat{I^P} m}{N} - \frac{\beta \hat{S^D} \hat{I^D}}{N} - \mu \hat{S^D} \tag{A.3}$$

$$\frac{d\hat{I^D}}{dt} = -\frac{\ln(\alpha) \hat{I^P} \hat{I^P} m}{N} + \frac{\beta \hat{S^D} \hat{I^D}}{N} - \mu \hat{I^D} \tag{A.4}$$

$$\frac{d\hat{R^D}}{dt} = \mu \left(\hat{I^D} + \hat{S^D} \right). \tag{A.5}$$

The differential equations of model (A) follow from the difference equations for the underlying Markov chain, and are natural. For example, intuitively, Equation (A.1) says that the predetection susceptible class decreases either through infection, which occurs instantaneously with probability $\frac{\beta I^P}{N}$, or detection, which occurs instantaneously with probability $-\frac{\ln(\alpha) S^P I^P m}{N}$. The other equations of model (A) can be derived and described similarly.

Figure 7 shows that this naive approach does not track the average state of the underlying Markov chain. Both the simulation and model (A) are parameterized with the same parameters as those in Figure 2. Across all state variables, the differential equation and the simulation begin in agreement, but later drift apart. Intuitively, this is because model (A) reaches states that can never be reached by the simulation. An accurate model requires more state—the unencumbered system that tracks the prethreshold progression—and explicit modeling of the sharp threshold event—the D variable. This intuition leads to the development of the method in Section 3, and results in the correct model presented as Equations (7).

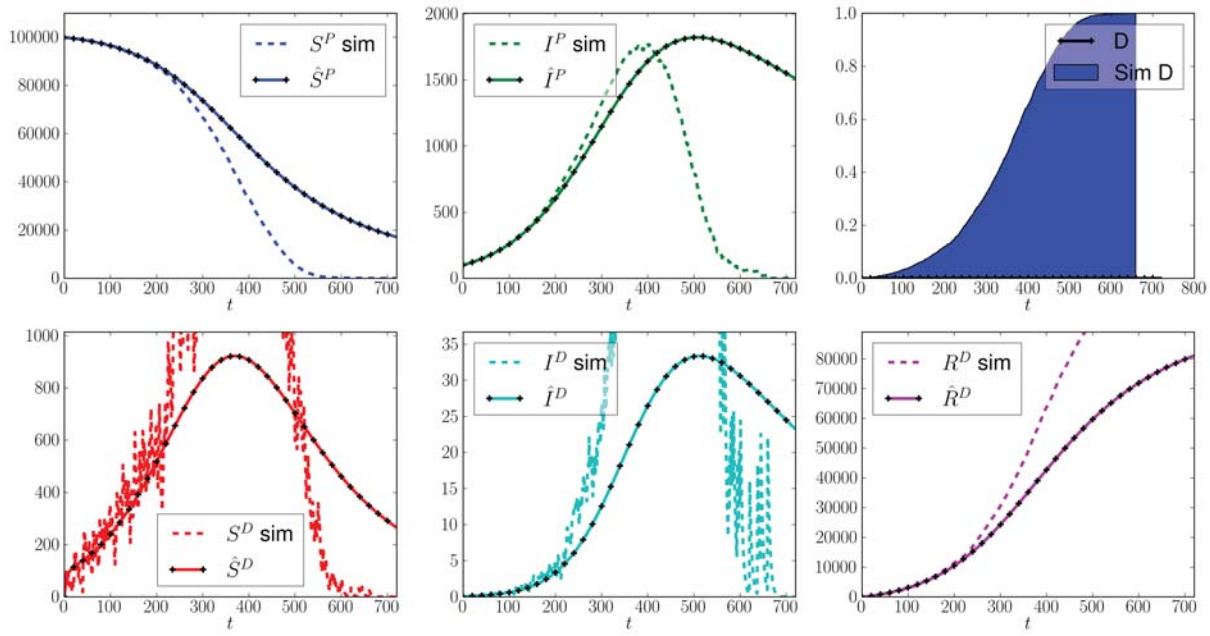


Figure 7: Comparison of simulation to naive cyber infection model. These figures parallel those of Figure 2. The simulation and the naive model, (10), are parameterized in the same way as the models in Figure 2. The naive approach simply does not hold a sufficient amount of state to accurately describe the evolution of the system. The simulation and the naive differential equation model begin in agreement, but quickly drift apart in all state variables.

B Solution of the D Equation

Equation (7c) is equivalent to

$$I^P(t) = (1 - D(t))I(t)$$

It is known that $I(t)$ has a closed solution,

$$I(t) = \frac{I_0 N}{I_0 + S_0 e^{-\beta N t}}.$$

For details see Daley and Gani, (1999). We use the equation for $I(T)$ to define $I^P(t)$ in terms of $D(t)$, and substitute the result into (7c) to get

$$\frac{dD}{dt} = \frac{-\ln(\alpha)m}{N}(1 - D)\frac{I_0 N e^{\beta N t}}{I_0 e^{\beta N t} + S_0}.$$

Separating variables gives

$$\frac{dD}{1-D} = \frac{-\ln(\alpha)m}{N}\frac{I_0 N e^{\beta N t}}{I_0 e^{\beta N t} + S_0}dt,$$

which is valid because $D(t) < 1 \; \forall_t$, and therefore $1 - D(t) > 0$. The key step is that both sides of this equation are of the form dU/U. We let $U = 1 - D$ and $V = I_0 e^{\beta N t} + S_0$ to derive

$$\frac{-dU}{U} = \frac{-\,ln(\alpha)m}{N\beta}\frac{dV}{V}.$$

Multiplying both sides by -1 and integrating gives

$$\ln(1-D) = \frac{\ln(\alpha)m}{N\beta}\ln(I_0 e^{\beta N t} + S_0) + C.$$

The above expression reduces to

$$D = 1 - \kappa\left[I_0 e^{\beta N t} + S_0\right]^{\frac{\ln(\alpha)m}{N\beta}},$$

where $\kappa = N^{\frac{-\ln(\alpha)m}{N\beta}}$ to ensure the initial condition $D(0) = 0$.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Research Sponsored Programs Office, Code 41
   Naval Postgraduate School
   Monterey, California

4. Richard Mastowski (Technical Editor).....1
   Graduate School of Operational and Information Sciences (GSOIS)
   Naval Postgraduate School
   Monterey, California

5. CDR Harrison Schramm.....1
   Graduate School of Operational and Information Sciences (GSOIS)
   Naval Postgraduate School
   Monterey, California

6. Assistant Professor Nedialko Dimitrov 1
   Graduate School of Operational and Information Sciences (GSOIS)
   Naval Postgraduate School
   Monterey, California

7. Dr. Jerry Smith.....1
   OPNAV N-81
   Navy Staff
   Arlington, Virginia